II. AMENDMENTS TO THE CLAIMS

The following listing replaces any and all prior listings of the claims:

1. (Currently amended) A computer-implemented security system for securing an electronic version of a nucleotide chain sequence, wherein the nucleotide chain sequence comprises at least a portion of a genome of an organism, the system comprising:

a computer hardware apparatus; and

a computer program that, when loaded and executed, controls the computer hardware apparatus such that it carries out:

identifying a sequence of at least one exon[[s]] and a sequence of at least one intron[[s]] in the nucleotide chain sequence;

selectively encrypting the sequence of only the at least one exon[[s]] identified in the nucleotide chain to provide security over a network; and

outputting the electronic version of the nucleotide chain sequence, including both the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]], wherein the encrypted sequence of the at least one exons are is subsequently decrypted by a secure process to regenerate the nucleotide chain sequence.

2. (Currently amended) The computer-implemented security system of claim 1, wherein the system for outputting further comprises a system for transmitting the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]].

3. (Currently amended) The computer-implemented security system of claim 2, wherein the ~~system for~~ transmitting of the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]] ~~includes~~ utilizes at least one XML document.

4. (Currently amended) The computer-implemented security system of claim 2, wherein the ~~system for~~ transmitting of the encrypted sequence of the at least one exon[[s]] and the sequence of the at least one unencrypted intron[[s]] ~~includes~~ utilizes web services.

5. (Currently amended) The computer-implemented security system of claim 1, wherein the ~~system for~~ selectively encrypting only the sequence of the at least one exon[[s]] utilizes cipher block chain encrypting.

6. (Currently amended) The computer-implemented security system of claim 2, wherein the computer program controls the computer hardware apparatus such that it further carries out ~~comprising~~:

   ~~a system for~~ receiving the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]];

   ~~a system for~~ decrypting the encrypted sequence of the at least one exon[[s]]; and

   ~~a system for~~ regenerating the nucleotide chain from the decrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]].

7. (Currently amended) The computer-implemented security system of claim 6, wherein the ~~system for~~ receiving the encrypted <u>sequence of the at least one</u> exon[[s]] and <u>the</u> unencrypted <u>sequence of the at least one</u> intron[[s]] comprises a bioinformatics database for receiving nucleotide chain queries.

8. (Currently amended) A method for transmitting a nucleotide chain sequence, wherein the nucleotide chain sequence comprises at least a portion of a genome of an organism, the method comprising:

identifying <u>a sequence of at least one</u> exon[[s]] and <u>a sequence of at least one</u> intron[[s]] in the nucleotide chain sequence;

selectively encrypting <u>the sequence of</u> only the <u>at least one</u> exon[[s]] identified in the nucleotide chain ~~to generate encrypted exons and unencrypted introns~~;

transmitting <u>the</u> encrypted <u>sequence of the at least one</u> exon[[s]] and <u>the</u> unencrypted <u>sequence of the at least one</u> intron[[s]];

receiving the encrypted <u>sequence of the at least one</u> exon[[s]] and <u>the</u> unencrypted <u>sequence of the at least one</u> intron[[s]];

decrypting the encrypted <u>sequence of the at least one</u> exon[[s]];

regenerating the nucleotide chain sequence from the decrypted <u>sequence of the at least one</u> exon[[s]] and unencrypted <u>sequence of the at least one</u> intron[[s]]; and

outputting the regenerated nucleotide chain sequence.

9. (Canceled)

10. (Previously presented) The method of claim 8, comprising the further step of querying a bioinformatics database with the received nucleotide chain sequence.

11. (Currently amended) The method of claim 8, wherein the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]] are transmitted in at least one XML document.

12. (Currently amended) The method of claim 8, wherein the encrypted sequence of the at least one exon[[s]] and the unencrypted sequence of the at least one intron[[s]] are transmitted using web services.

13. (Currently amended) The method of claim 8, wherein the step of selectively encrypting the sequence of only the at least one exon[[s]] utilizes cipher block chain encrypting.

14. (Currently amended) A program product stored on a recordable medium for encoding a nucleotide chain sequence, wherein the nucleotide chain sequence comprises at least a portion of a genome of an organism, the program product comprising:

   means for identifying a sequence of at least one exon[[s]] and a sequence of at least one intron[[s]] in the nucleotide chain sequence;

means for selectively encrypting only the <u>sequence of the at least one</u> exon[[s]] identified in the nucleotide chain sequence to provide security over a network; and

means for outputting the <u>nucleotide chain sequence including both the</u> encrypted <u>sequence of the at least one</u> exon[[s]] and the ~~non-~~unencrypted <u>sequence of the at least one</u> intron[[s]] over the network, wherein the encrypted <u>sequence of the at least one</u> exon~~s are~~ <u>is</u> <u>subsequently</u> decrypted by a secure process to regenerate the nucleotide chain sequence.

15. (Currently amended) The program product of claim 14, wherein the encrypted <u>sequence of</u> <u>the at least one</u> exon[[s]] and unencrypted <u>sequence of the at least one</u> intron[[s]] are stored in at least one XML document.

16. (Currently amended) The program product of claim 14, wherein the means for selectively encrypting only the <u>sequence of the at least one</u> exon[[s]] utilizes cipher block chain encrypting.

17. (Currently amended) A program product stored on a recordable medium for decoding an encoded nucleotide chain, wherein the nucleotide chain sequence comprises at least a portion of a genome of an organism, the method comprising:

means for identifying <u>an</u> encrypted <u>sequence of at least one</u> exon[[s]] and <u>an</u> unencrypted <u>sequence of at least one</u> intron[[s]] in the encoded nucleotide chain sequence;

means for selectively decrypting only the <u>sequence of the at least one</u> exon[[s]] identified in the encoded nucleotide chain sequence;

means for reassembling the <u>sequence of the at least one</u> exon[[s]] and <u>the sequence of the at least one</u> intron[[s]] to generate a decoded nucleotide chain sequence; and

means for outputting the decoded nucleotide chain sequence.

18. (Currently amended) The program product of claim 17, wherein the <u>sequence of the at least one</u> exon[[s]] and <u>the sequence of the at least one</u> intron[[s]] are stored in at least one XML document.

19. (Currently amended) The program product of claim 17, wherein the means for selectively decrypting only the <u>sequence of the at least one</u> exon[[s]] utilizes cipher block chain decrypting.

20. (Previously presented) The program product of claim 17, further comprising means for querying a bioinformatics database with the decoded nucleotide chain sequence.